


CLAIMS

What is claimed is:

- Sub
B1
1. In a computer system, a method for securing access to data, comprising:
- generating a first message at a first computer system, said first message comprising information corresponding to data, and transmitting said first message to a second computer system;
 - receiving said first message at said second computer system, and generating a key pair comprising an encode key and a decode key for encoding and decoding of said data;
 - generating a second message comprising the encode key, and transmitting said second message to said first computer system; and
 - receiving said second message at said first computer system, wherein said encode key in the second message can be used to encode said data.
2. The method of claim 1 further comprising:
- storing said key pair and said information in said first message in a record;
3. The method of claim 1, further comprising encoding said data using said encode key, and storing said encoded data.

 4. The method of claim 1, wherein said first computer system comprises at least one client computer system and said second computer system comprises at least one server computer system.

5. The method of claim 1, wherein said step of generating said first message further comprises:

generating a one way hash function of said data; and
placing said hash function, information identifying said data, and user information for a user of said data at said first computer system in said first message.

6. The method of claim 5, further comprising:

obtaining said first message at said second computer; generating a time stamp, and a digital signature representing said digital time stamp and said hash function in said first message; and storing said user information, said information identifying said data, hash function, said time stamp and said digital signature in said record.

7. The method of claim 6 wherein said second message further comprises:

said time stamp, said information identifying said data, and said digital signature in said second message.

~~8~~

8. The method of claim 1, further comprising:
providing access to encoded data by performing steps comprising:
generating a third message at said first computer system, said
third message comprising information corresponding to said encoded data, and
transmitting said third message to said second computer system;
receiving said third message at said second computer system, and
using said information in said third message to retrieve a record corresponding
to said encoded data, said record including a decode key for decoding said
encoded data;
generating a fourth message comprising said decode key, and
transmitting said fourth message to said first computer system;
receiving said fourth message at said first computer system,
wherein said decode key in said fourth message can be utilized to decode said
encoded data.

9. The method of claim 8, further comprising;
accessing said encoded data and decoding said encoded data using
said decode key.

10. The method of claim 8, wherein said third message further
comprises:



said information identifying said encoded data, said user information, and said digital signature.

11. The method of claim 10, further comprising:
receiving said third message at said second computer system;
accessing said corresponding record; and
verifying said digital signature therein with said received digital signature.
12. The method of claim 11, further comprising:
upon proper verification, generating a fourth message comprising information identifying said encoded data file and said decode key, and transmitting said fourth message to said first computer.
13. The method of claim 12, further comprising:
receiving the fourth message at the first computer;
accessing the encoded data;
and using said decode key in said fourth message to decode said encoded data.
14. The method of claim 11, further comprising:



upon successful verification, generating a data retrieval time stamp and storing said data retrieval time stamp in a corresponding record.

15. The method of claim 14, further comprising:

upon unsuccessful verification, generating an attempted data retrieval time stamp and storing said attempted data retrieval time stamp in said corresponding record.

16. In a network system a method of providing access to encoded data, comprising:

generating a first message at a first computer system, said first message comprising information corresponding to said encoded data, and transmitting said first message to a second computer system;

receiving said first message at said second computer system, and using said information in said first message to retrieve a record corresponding to said encoded data, said record comprising a decode key for decoding said encoded data;

generating a second message comprising said decode key, and transmitting said second message to said first computer system;

receiving said second message at said first computer system, wherein said decode key in said second message can be utilized to decode said encoded data.



17. The method of claim 16 further comprising;
accessing said encoded data and decoding said encoded data using
said decode key.

18. The method of claim 16 wherein said first computer system
comprises at least one client computer system and said second computer
system comprises at least one server computer system.

19. A system for securing access to data, comprising a first computer
system interconnected to a second computer system via a communication link,
wherein said first and said second computer systems are configured to perform
steps comprising:

generating a first message at said first computer system, said first
message comprising information corresponding to said data, and transmitting
said first message to said second computer system;

receiving said first message at said second computer system, and
generating a key pair comprising an encode key and a decode key for encoding
and decoding of said data;

storing said decode key in a record;

generating a second message comprising said encode key, and
transmitting said second message to said first computer system; and



receiving said second message at said first computer system, wherein said encode key in said second message can be used to encode said data to secure access to said data.

20. The system of claim 19, wherein said first computer is further configured to use said encode key to encode said data, and store said encoded data.

21. The system of claim 19, wherein said first and said second computer systems are further configured for providing access to encoded data by performing steps comprising:

generating a third message at said first computer system, said third message including information corresponding to said encoded data, and transmitting said third message to second computer system;

receiving said third message at said second computer system, and using said information in said third message to retrieve a record corresponding to said encoded data, said record including a decode key for decoding said encoded data;

generating a fourth message comprising said decode key, and transmitting said fourth message to said first computer system;

receiving said fourth message at said first computer system, wherein said decode key in said fourth message can be utilized to decode said encoded data.

~~Handwritten signature~~

22. The system of claim 21, wherein said first computer is further configured to access said encode data and use said decode key to decode said encoded data.

~~Handwritten signature~~

005259-62064560